Amendments to the Claims

1. (currently amended) A link lock system for a network, comprising:

a computer;

a network interface device to provide the computer with access to the network;

a bus monitor to monitor a first link between the network interface device and the computer, where ~~said~~ the bus monitor reports detected failures or intrusions; and

a security switch to switch the first link from a non-secured mode using an HTTP protocol to a secured mode using an HTTP-S protocol when a report of ~~said~~ the detected failures or intrusions is received from the bus monitor.

2. (currently amended) The system of claim 1, wherein ~~said~~ the computer is a server.

3. (currently amended) The system of claim 1, wherein the network operates in ~~a~~ the secured mode using ~~an~~ the HTTP-S protocol.

4. (cancelled)

5. (cancelled)

6. (currently amended) The system of claim 1, further comprising:

a controller that receives the report from the bus monitor and sends a control signals to the network interface device, the security switch, and the computer.

7. (currently amended) The system of claim 6, further comprising:

an encryption element in the computer, where ~~said~~ the encryption element converts data placed on ~~said~~ the first link ~~to a~~ using the secured protocol when the control signal is received from ~~said~~ the controller.

8. (currently amended) A system for a server, comprising:

an interface device to provide the server with access to a network; and

a controller to monitor a link between the interface device and the server, where ~~said~~ the controller switches the link from a non-secured protocol using an HTTP protocol to a secured protocol using an HTTP-S protocol when failures or intrusions are detected on the link.

9. (currently amended) The system of claim 8, wherein the network is the Internet~~, such that the non-secured protocol includes HTTP, and the secured protocol includes HTTP-S~~.

10. (currently amended) The system of claim 8, wherein ~~said~~ the controller sends a control signal to the server when failures or intrusions are detected on the link.

11. (currently amended) The system of claim 10, further comprising:

an encryption element in the server, where ~~said~~ the encryption element converts data placed on ~~said~~ the link by the server ~~to~~ using ~~a~~ the secured protocol when the control signal is received from ~~said~~ the controller.

12. (currently amended) A method, comprising:

monitoring a link between a network device and a computer;

first directing the link to use an HTTP-S secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to an HTTP non-secured protocol when ~~said~~ the detected failures or intrusions have been corrected.

13. (cancelled)

14. (cancelled)

15. (original) The method of claim 12, wherein the computer is a server.

16. (currently amended) An apparatus comprising a machine-readable storage medium having executable instructions that enable the machine to:

monitor a link between a network device and a server;

first directing the link to use an HTTP-S secured protocol when failures or intrusions are detected on the link; and second directing the link to revert to an HTTP non-secured protocol when ~~said~~ the detected failures or intrusions have been corrected.

17. (cancelled)

18. (cancelled)

19. (new) The method of claim 12, wherein the link reverts to the HTTP non-secured protocol when a network manager determines that the detected failures or intrusions have been corrected.

20. (new) The apparatus of claim 16, wherein the link reverts to the HTTP non-secured protocol when a network manager determines that the detected failures or intrusions have been corrected.